3Com HomeConnect ADSL Modem Ethernet CLI User’s Guide

Version 1.0

**3Com Corporation
3800 Golf Road
Rolling Meadows, IL
60008**

3Com Corporation reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of 3Com Corporation to provide notification of such revision or change.

3Com Corporation provides this documentation without warranty of any kind, either implied or expressed, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. 3Com may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

UNITED STATES GOVERNMENT LEGENDS:

If you are a United States government agency, then this documentation and the software described herein are provided to you subject to the following:

United States Government Legend: All technical data and computer software is commercial in nature and developed solely at private expense. Software is delivered as Commercial Computer Software as defined in DFARS 252.227-7014 (June 1995) or as a commercial item as defined in FAR 2.101(a) and as such is provided with only such rights as are provided in 3Com's standard commercial license for the Software. Technical data is provided with limited rights only as provided in DFAR 252.227-7015 (Nov 1995) or FAR 52.227-14 (June 1987), whichever is applicable. You agree not to remove or deface any portion of any legend provided on any licensed program or documentation contained in, or delivered to you in conjunction with, this User Guide.

YEAR 2000 INFORMATION:

For information on Year 2000 compliance and 3Com products, visit the 3Com Year 2000 web page:

http://www.3Com.com/products/yr2000.html

1 Accessing the Configuration Interface

2 CLI Command Conventions and Terminology

3 Manual setup

4 FILTERING CAPABILITIES

5 Upgrading 3Com HomeConnect ADSL Modem Ethernet Operational Software

A CLI Command Description

Technical Support and Limited Warranty

1 ACCESSING THE CONFIGURATION INTERFACE

This chapter explains how to attach to the configuration interface locally via the console port or remotely via a Telnet session. This chapter also introduces you to the capabilities and conventions associated with management of your 3Com HomeConnect ADSL Modem Ethernet.

Establishing Communications

Local Connection

If you want to attach locally to the 3Com HomeConnect ADSL Modem Ethernet via the console (serial) port, you will need to connect the supplied serial cable to the Console Port located on the unit and the Serial Port on your computer. In addition, you will also need a terminal emulation program appropriate for your computer. See the following subsections for various emulation options.

No matter which emulator you use, configure your settings to:

- 9600 baud
- 8 data bits
- no parity
- 1 stop bit
- direct connect

IBM-PC Compatible Computers

Windows Terminal (included with Microsoft Windows 3.x) and ProComm Plus are popular communications packages which support VT100 terminal emulation for IBM-PC compatible computers. HyperTerminal, bundled with Windows 95 and 98, also provides terminal emulation.

Macintosh Computers

ProComm, MicroPhone, White Knight, Kermit, Red Ryder, VersaTerm and ZTerm (a shareware application available on the Internet and many online services) are popular communications programs which carry vt100 terminal emulation service for Macintosh computers. If you don’t have a communications package or your program doesn’t support vt100 emulation, ZTerm will function just as well.

UNIX-Based Computers

Kermit, minicom and tip are typical terminal emulation programs for UNIX-based computers. Depending on the platform you’re using, you may need to modify a configuration file for vt100 settings.

Remote Connection

If you want to attach to the 3Com HomeConnect ADSL Modem Ethernet via the LAN or WAN interface of the unit, you will need to establish a Telnet connection to the unit.

The 3Com HomeConnect ADSL Modem Ethernet must have an IP address and an administrative login profile (username and password) in order to connect to it with Telnet. The IP address and administrative login profile are automatically created when the unit is initially configured using the IP Wizard. The default username is 'root' and the default password is '!root'. Refer to the Chapter 3 for how to use the IP Wizard to assign an IP address to the unit. Alternatively, the IP address and administrative login profile can be created using CLI commands.

From Windows 95, you can go to the DOS Window and run:

```
telnet <ip_address>
```

This will bring up the login prompt for the unit. Once you have successfully logged in, the Command Line Interface presentation is the same as if you were locally attached.

*When you want to terminate your Telnet session, type **quit** at the CLI prompt.*

2

CLI Command Conventions and Terminology

This chapter describes the command syntax, conventions and terminology used within the Command Line Interface. Reviewing and understanding this chapter is essential for you to understand subsequent chapters.

Command Structure

Format

Commands can be followed by values and/or parameters and values. For example:

add ip network <network_name> address [ip_addr]

- **add ip network** is the command
- *<network_name>* is the (required) value for the command
- **address** is a required parameter
- *[ip_addr]* is the value for the IP address parameter which you must provide

Parameters

- are order independent
- **{ … }** parameters enclosed by curly braces are required, and are provided with default values. You do not need to specify these parameters unless you wish to override the default.

Values

- **< … >** required values for a command or parameter are enclosed by arrows.
- **[…]** range of values following parameters are enclosed in brackets. Inside the brackets, if you see a:
- **| (**vertical bar) you may select only *one* of the displayed choices:
  [FIRST **|** SECOND **|** THIRD]
- **,** (comma) you can select *one or more* of the displayed choices:
  [FIRST,SECOND,THIRD,...]

The type of value you enter must match the type requested. Numbers are either decimal or hexadecimal. Text can be either a string that you create, or it may be a list of options you must choose from. When choosing an option, type the text of the option exactly.

Names or Strings

"Double quotation marks" set off user-defined strings. If you want white space or special characters in a string, it must be enclosed by "double quotation marks".

Network Address Formats

Many commands require a network address, to define a link to a remote host, workstation or network. Network addresses are shown in this document using the syntax described in the following table:

Address Type	Format	Range
IP_address	a.b.c.d	0.0.0.0 to 255.255.255.255 (decimal)
ip_net_address	a.b.c.d/mask	255.255.255.255/A,B,C,H
mac_address	xx:xx:xx:xx:xx:xx	hexadecimal pairs

Abbreviation and Command Completion

- Commands can be *abbreviated* if arguments you write are unique.
  For example, **se po 2 vc 33**, short for: **set port 2 vci 33** is acceptable, but **se po 2 v 33** isn't unique because **v** can stand for **vpi** or **vci**.
- As a convention, some commands illustrated in this manual are abbreviated and annotated as such *(abbr.)* for brevity.
  Also*, s*ome parameters are omitted in examples because they default to standard values and do not require entry, or are unnecessary for common configuration. See the *CLI Reference* section for more details.
- *Command completion* finishes spelling a unique, abbreviated parameter for you just by pressing the key. It's handy when you're in a hurry or uncertain about a command. For example, if you type **add ip n[ESC]**, it will spell out the keyword **network** without losing your place in the command syntax.

Control Characters

- Commands can be *retrieved* by typing **<ctrl>P** [^P] (for previous) and **<ctrl>n** [^n] (for next). Command retrieval consults the *history* of previous fully entered commands, defaulting at the last ten commands. If an error occurs while a command is processing, any partial command (up to and including the field in error) is added to the history list.
- The current command can be *killed* by pressing **<ctrl>C** [^C].
- A partially completed command line can be *reprinted* - a useful function if, due to interrupted output, you're unsure what 3Com HomeConnect ADSL Modem Ethernet has "seen" up to now - by pressing **<ctrl>L** [^ L] (for last).

Help

- Help is *general* or *positional*. Type **help <any command**> to get a cursory list of associated commands and its syntax. Type **<any command> ?** to get more extensive, positional help for a particular field. Help is most useful *during* configuration: query the list of possible parameters by typing **?** and, when you find the value you need, type it without losing your place in the argument. Just be sure to leave a space between the keyword and the question mark.

Conventions

- Most commands are *not* case sensitive. As a rule, only <*name*> and *[password]* values require typing the correct case.
- Configuration changes **are lost on reboot unless you save them.** The **save all** command places configuration changes in FLASH ROM (permanent memory). The changes are lost if not saved to FLASH ROM or if power is lost before you can save them.
- Commands to change most bridge port settings do not take effect until the port has been disabled and re-enabled.

Command Language Terminology

The CLI command language creates, manages, displays and removes system entities. These entities describe system and network connections and processes. Most of the managed entities in the system are slotted in tables. Some common examples are:

- **Network** - defines local and remote networks, network connections, hosts and routers
- **Port** - A table of parameters that describes the characteristics of a bridge port. These parameters are used when establishing a network connection over the WAN
- **User** - A table of parameters that describes connection parameters associated with Telnet users that wish to attach and remotely manage the unit
- **Filter** - can be applied to interfaces, connections, and theernet port to control access through the system
- **Interface** - describes physical devices; for example, ports
- **Route** - describes a path through the network to another system or network

Table entries are created with an **add** command, and removed with a **delete** command. The **add** command specifies the most important parameters of the entry. Additional parameters are usually specified with the **set** command, which is also used to change configured parameters.

The **list** command displays table entries. For example, **list users** displays all defined administrative login profiles.

The **show** command displays detailed information about a specific table entry. For example, **show user root** displays detailed information for the administrative login profile *root*.

3

MANUAL SETUP

This chapter describes how to manually setup the 3Com HomeConnect ADSL Modem Ethernet.

Configuration Overview

A bridge connects two or more physical networks together to function as a single, large network. The 3Com HomeConnect ADSL Modem Ethernet is a learning bridge. A learning bridge does more than just link networks; it separates network traffic and forwards only the packets that need to be forwarded.

Bridges separate traffic by examining the Media Access Control (MAC) addresses contained in data packets. MAC addresses uniquely identify each machine attached to a network segment. A data packet is not forwarded to another segment if its destination MAC address resides on the same segment as its source.

To efficiently separate traffic, the bridge maintains a Bridge Forwarding Table. The table contains a list of MAC addresses and their associated network segments. The table is built dynamically from the source MAC addresses of data packets passing through the bridge.

The 3Com HomeConnect ADSL Modem Ethernet bridge supports the Spanning Tree Protocol (STP). This feature is used when two networks are joined by two bridges forming a looped network. STP prevents the data packets from circling the two networks.

The 3Com HomeConnect ADSL Modem Ethernet is a 9-port bridge with a single ethernet port on the Ethernet physical interface (named *eth:1*) and 8 ATM PVCs (WAN ports) through the ATM/ADSL physical interface (named *atm:1*). Bridge ports are numbered 1through 9, with the Ethernet port designated as port 1. By default, packets are not bridged between the WAN ports.

The rest of this chapter provides an overview of the 3Com HomeConnect ADSL Modem Ethernet basic operations and configuration. The chapter is broken into the following sections:

- Bridge Port Management
- Advanced Bridging
- IP Access
- System Administration

Managing Bridge Ports

Each Bridge WAN Port (2-9) has an associated profile for storing information about the port. With this profile, you specify ATM Virtual Channel information, description information and whether the port is currently enabled or disabled.

You modify the profile using *set port* commands to setup the WAN connection and network information.

Remember to save your configuration using the ***save all*** *command before rebooting your 3Com HomeConnect ADSL Modem Ethernet so that your changes will be written to permanent FLASH memory.*

- You can obtain a list of all currently configured port profiles using the command:

  ```
  list ports
  ```

- You can view the contents of a particular profile using the command:

  ```
  show port <port_number>
  ```

The 3Com HomeConnect ADSL Modem Ethernet always has a *default* profile. Any value that is not set in a profile that you create will assume the values that are present in the *default* profile.

- You can view the *default* profile using the command:

  ```
  show port default
  ```

Bridge port profiles can be enabled or disabled. When a port is enabled using the *enable port* command, the 3Com HomeConnect ADSL Modem Ethernet reads the connection parameters for the port from the profile and establishes a connection. When a port is disabled using the *disable port* command, the connection will be terminated and no other data will be directed out the bridge port. Configuration changes to a bridge port profile do not take effect until the next time the profile is enabled. Thus, if you want to make changes to the profile you should disable the profile, make your changes, and then re-enable the profile.

- For example, if you want to change the VCI value to 35 for bridge port 2:

  ```
  disable port  2
  set port 2 vci 35
  enable port 2
  ```

Configuring ATM Information

The 3Com HomeConnect ADSL Modem Ethernet bridges packets over ATM virtual circuits. ATM allows for permanent connections (PVCs) and switched connections (SVCs). Each PVC is identified by its Virtual Path and Connection Identifiers (VPI/VCI). The VPI/VCI uniquely specifies a path to a remote site and is placed in the ATM cell header that is used to route each cell through the network.

Two ports with the same VPI and VCI can not be enabled simultaneously. You should disable all ports that use the same VPI/VCI and then enable the one that should be active.

For SVCs, there is not a fixed VPI/VCI. Instead, a destination address is used to set up a path through the ATM backbone network when the connection is to be established.

Currently, the SVC capability is disabled in the 3Com HomeConnect ADSL Modem Ethernet. The VPI/VCI values to use for a bridge port are specified using the 'set port' command:

```
set port <port_number> vci <vci_value> vpi <vpi_value>
```

The 3Com HomeConnect ADSL Modem Ethernet supports Unspecified Bit Rate (UBR) traffic. The modem will normally attempt to use all of the available upstream bandwidth when transmitting data. Optionally, on a bridge port basis, the upstream traffic can be 'shaped' to use only a portion of the available bandwidth using the Peak Cell Rate parameter.

The Peak Cell Rate is specified in cell-per-second. Use the following formula to determine the Peak Cell Rate to enter for a given throughput.

pcr_value = throughput / 3392

where:

throughput is the desired transmit rate in bits/second.

- To set the Peak Cell Rate use the command:

```
set port <port_number> pcr <pcr_value>
```

Advanced Bridging

Remember to save your configuration using the ***save all*** *command before rebooting your 3Com HomeConnect ADSL Modem Ethernet so that your changes will be written to permanent FLASH memory.*

Advanced Bridging Settings

Bridging is globally enabled by default, to disable bridging use the **disable bridge forwarding** command**.**

The advanced bridging configuration options include Aging Time, Forward Delay, Spanning Tree, and Spanning Tree Priority.

- To see the current settings for these options, use the command:

```
show bridge
```

Except for enabling Spanning Tree, most users do not need to change the advanced parameters from their default settings.

The Aging Time is the time (in seconds) for aging out forwarding table information.

- To change the Aging Time, use the command:

```
set bridge aging_time <seconds>
```

The Forward Delay is the time (in seconds) to wait while learning forwarding information before starting to bridge packets.

- To change the Forwarding Delay, use the command:

```
set bridge forward_delay <seconds>
```

The Spanning Tree Protocol is used to eliminate network loops between bridges.

- To disable or enable Spanning Tree, use the commands:

```
disable bridge spanning_tree or
enable bridge spanning_tree
```

The Spanning Tree Priority is the priority assigned to a bridge that is running the Spanning Tree Protocol. It is used for prioritizing the bridges when Spanning Tree is enabled.

- To change the Spanning Tree Priority, use the command:

```
set bridge spanning_tree_priority <priority value>
```

Restricting LAN Access

Access to the bridging functions of the 3Com HomeConnect ADSL Modem Ethernet can be restricted to certain MAC addresses by using the Access MAC Address feature. When enabled, only packets sourced by or destined for workstations with MAC addresses in the Access MAC Address Table will be bridged.

- To add a MAC address to the Access MAC Address Table, use the command:

```
add bridge access_mac_address <mac _addr>
```

Note: *the mac address should be entered in the form: xx.xx.xx.xx.xx.xx*

- To delete a MAC address from the Access MAC Address Table, use the command:

```
delete bridge access_mac_address <mac _addr>
```

- To enable the use of the Access MAC Address feature, use the command:

```
enable bridge access_mac_addresses
```

- To disable the use of the Access MAC Address feature, use the command:

```
disable bridge access_mac_addresses
```

Canned Filters

The 3Com HomeConnect ADSL Modem Ethernet provides sophisticated generic filtering capabilities. Normally, filters must be created with a text editor, copied to the unit, and applied to the appropriate interface or bridge port. This process is described in the chapter on Filtering.

To simplify this process, several pre-programmed filters installed in the unit. These “canned” filters allow or restrict certain common protocols from being transported over a Bridge WAN port. The filters can be applied to a Bridge WAN port with a single command.

The following canned filters are pre-programmed:

Table 3-1 Pre-Programmed Filters

Filter Name	Function
NO_IP	Do not allow IP packets
NO_IPX	Do not allow IPX packets
NO_IP_IPX	Do not allow IP or IPX packets
ONLY_IP	Only allow IP packets
ONLY_IPX	Only allow IPX packets
ONLY_IP_IPX	Only allow IP or IPX packets
ONLY_PPPOE	Only allow PPP-Over-Ethernet packets

- To apply a canned filter to a bridge port, use the command:

```
set port <port_number> filter <filter_name>
```

- To disable port filtering, use the command:

```
set port <port_number> filter none
```

IP Configuration

To allow remote SNMP and Telnet management of the 3Com HomeConnect ADSL Modem Ethernet you must configure the unit's IP stack. The IP stack can receive packets from any bridge port.

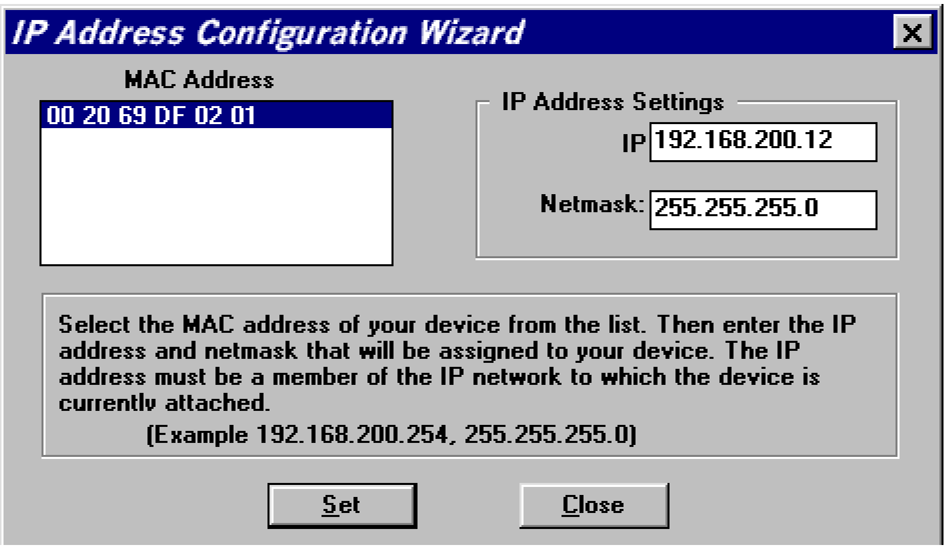
*Remember to save your configuration using the **save all** command before rebooting your 3Com HomeConnect ADSL Modem Ethernet so that your changes will be written to permanent FLASH memory.*

IP Wizard

The IP Wizard is designed to help you assign a specific IP address to your unit.

In order to manage the 3Com HomeConnect ADSL Modem Ethernet, the unit must be assigned an IP address. You must also have an administrative login profile (user name and password) assigned.

To access the IP Wizard, go to **Start > Programs > 3Com HomeConnect ADSL Modem Ethernet**, and click on "**IP Wizard**".



MAC Address

00 20 69 DF 02 01

IP Address Settings

IP 192.168.200.12

Netmask: 255.255.255.0

Select the MAC address of your device from the list. Then enter the IP address and netmask that will be assigned to your device. The IP address must be a member of the IP network to which the device is currently attached.

(Example 192.168.200.254, 255.255.255.0)

IP Wizard will search the LAN for all unconfigured 3Com HomeConnect Modems. As each unconfigured unit is found, the unit's MAC address is placed in the selection box. For multiple HomeConnect modems, you can determine which MAC address belongs to the one you want to configure by disconnecting the HomeConnect's Ethernet cable and running IP Wizard again. The missing MAC Address belongs to that unit.

Select which HomeConnect Modem you want to configure and enter its LAN IP address and netmask; then press **Set**.

*If you assign the IP address with the IP Wizard, the administrative login name is **root** and the password is **!root**. **After you access the unit, you are strongly advised to delete this login profile and create a new one with a secure***

name and password. *(Maximum character length of login name = 32, password maximum character length = 15.)*

Configuring an IP Network

The 3Com HomeConnect ADSL Modem Ethernet can have more than one IP address (i.e., belong to more than one IP network). To configure an IP address use the *add ip network* command. Each network has a *network name*. You will use the *network name* when entering commands related to the network.

The CIDR-supported *network address* includes a local station address and subnet mask using the format: *nnn.nnn.nnn.nnn/A B C* or *8-30*. The first 4 octets describe the IP address, followed by the subnet mask (contiguous) designator.

You can specify the subnet in one of two ways: a class or numerical designation. If you specify a Class C subnet mask, for instance, this command will generate a 255.255.255.0 subnet value for you. If you specify the number of bits (to be set to 1), the acceptable range is 8-30. The network address is invalid if the portion of the station address not covered by the mask is 0.

Defining a numerical subnet is useful when your value falls in between classes. You can also *omit* the mask altogether; it will automatically be calculated from the address.

- To add an IP network, use the command:
  add ip network <network name>
  address <ip address/mask>
  frame [ETHERNET_II | SNAP]
- To list the defined IP networks, use the command

  ```
  list ip networks
  ```
- By default, the network is enabled when it is created. You can disable the network using the following command:

  ```
  disable ip network <network name>
  ```
- You can delete a disabled network using the command:

  ```
  delete ip network <network name>
  ```

The *reconfigure ip network* command can be used to modify an existing IP network's address or frame type.

Configuring Static Routes

A Static route is a configured route that will remain in the IP routing table until deleted.

- To add a Static route over the LAN, use the command:

```
add ip route <ip network address>
     gateway <ip address>
        metric <metric>
```

The route will appear in the IP routing table. You can display all IP routes with the **list ip routes** command.

To add a default route, use the command:

```
add ip default route
   gateway <ip_address>
   metric <metric>
```

The route will appear as destination 0.0.0.0 in the IP routing table.

- To delete an IP Static route, use the command:

  ```
  delete ip route <ip network address>
  ```

Configuring DNS

You can configure the 3Com HomeConnect ADSL Modem Ethernet to access a DNS server to resolve host names. This facility is used by the **ping, telnet, rlogin** and **update software ftp** commands.

DNS server entries are stored in the DNS Server Table.

To add a DNS server use the command:

```
add dns server <domain_name>
   primary <ip_addr>
   secondary <ip_addr>
```

The **<domain_name>** parameter can be a specific domain (i.e., 3com.com) or it can be the wildcard character '*', representing all domains. You can specify different DNS servers for different domains. When searching for the appropriate DNS server, the modem first searches the local DNS server table for a entry for the specific domain of the host name you are attempting to resolve. If no specific entry is found, the wildcard entry is used.

To list the entries in the DNS Server Table use the command:

```
list dns servers
```

To delete an entry from the DNS Server Table use the command:

```
delete dns server <domain_name>
```

where domain name is the specific domain or the wildcard character '*'.

IP Tools

The 3Com HomeConnect ADSL Modem Ethernet CLI provides a standard set of IP utility programs including Ping, TELNET and RLOGIN.

System Administration

This section provides details and examples for performing the following system administration tasks:

- Setting Date and Time
- Setting System Identification
- Configuring TELNET Login Access
- Providing TFTP Access
- Setting Password Protection
- Configuration Scripting

*Remember to save your configuration using the **save all** command before rebooting your 3Com HomeConnect ADSL Modem Ethernet so that your changes will be written to permanent FLASH memory.*

Setting Date and Time

You can obtain the current date, time and system uptime using the command:

```
show date
```

The date and time information is provided in the following format:

```
System Date:    02-MAR-1998 05:17:00
System UpTime:  2d 08:37:54
```

You can set the date using the command: **set date** which sets the system date, and leaves the time unchanged. The format is: dd-mmm-yyyy. The month should be the first three characters of the month name. The year can be either 2 or 4 digits - 99 or 1999. Example: **set date 01-JAN-1999**

To set the time, use the command: **set time** which sets the system time, and leaves the date unchanged. The format is: hh:mm:ss. The seconds (ss) field is optional. Military time is used. For example, to set the time to 4:10 am enter the command: **set time 04:10** and to set the time to 4:10 pm enter the command: **set time 16:10**.

Date and time settings are not maintained over a system reboot.

Setting System Identification

The system name, location and contact information is useful when monitoring the 3Com HomeConnect ADSL Modem Ethernet remotely. You should choose a name, location and contact that is appropriate for the unit.

- You can view the settings using the command:

  ```
  show system
  ```

- To set these parameters use the command:

  ```
  set system name <name> location <location> contact <contact>
  ```

- The name, location, and contact can be up to 32 characters long. For example,

  ```
  set system name Modem1 location Rack4 contact SysAdmin@555-1212
  ```

Configuring TELNET Login Access

Setting up a login user allows you to provide controlled access to the 3Com HomeConnect ADSL Modem Ethernet through TELNET. Connecting using TELNET on a workstation allows you to remotely manage the unit using CLI.

A default user name of **root** and password **!root** are provided by the IP Wizard during the initial installation. For secure access, you should add a private login name and password and delete the default name.

- To view the current login users, use the command:

  ```
  list users
  ```

- To add a login user, use the command:

  ```
  add user <name> password <password>
  ```

The name can be up to 32 characters long and the password can be up to 15 characters long.

- To delete a login user, use the command:

  ```
  delete user <name>
  ```

- To change the password, use the command:

  ```
  set user <name> password <new password>
  ```

- To enable the use of CLI for TELNET users, issue the additional command:

  ```
  enable security_option remote_user administration
  ```

Providing TFTP Access

Trivial File Transfer Protocol (TFTP) provides a simple way to transfer files from one machine to another. The 3Com HomeConnect ADSL Modem Ethernet has a TFTP server that allows you to copy files to or from the unit. All you have to do is set up TFTP access on the 3Com HomeConnect ADSL Modem Ethernet and run a TFTP client program on a workstation.

You can configure the 3Com HomeConnect ADSL Modem Ethernet to provide access to all TFTP clients or you can specify the IP addresses of the TFTP clients for restricted access.

- To view the current TFTP client access list, use the command:

  ```
  list tftp clients
  ```

- To add a TFTP client to the list, use the command:

  ```
  add tftp client <host name or IP address or 0.0.0.0>
  ```

Provide either the host name or the IP address of the workstation running the TFTP client. An address of 0.0.0.0 allows all TFTP clients unrestricted access.

- To remove a TFTP client from the list, use the command:

  ```
  delete tftp client <host name or IP address or 0.0.0.0>
  ```

Setting Password Protection

The 3Com HomeConnect ADSL Modem Ethernet provides the capability to password-protect access to the CLI. When the password protection feature is enabled, a user connecting to the CLI via the serial console port will be prompted for the CLI password.

After the correct password is entered, all CLI commands are accessible by the user. The user can 'exit' from the CLI to disable further access or can configure an idle timeout period. If no commands are executed by the CLI for a period longer than the idle timeout period, the user will automatically be logged out of the console. The password will have to be re-entered in order to access the CLI again.

CLI password protection is **disabled** by default.

Password protection can be configured by the QuickSetup program or by using CLI commands.

- To enable or disable CLI password protection, use the commands:

  ```
  set  command login_required yes             or
  set command login_required no
  ```

- To configure the login password, use the command:

  ```
  set command password <password>
  ```

- where ***<password>*** is an alphanumeric string of 1 to 8 characters. The default password is "password."

Be sure to save your configuration after entering a new password.

- After logging in to the CLI, you can exit the CLI with the command:

  ```
  exit cli
  ```

- To set the idle timeout period, use the command:

  ```
  set command idle_timeout <timeout>
  ```

- where <*timeout*> specifies the idle timeout period in minutes.
  By default, there is no idle timeout period.

Note: This capability is useful for system administrators or users who wish to restrict access to the 3Com HomeConnect ADSL Modem Ethernet.

Care should be taken to remember the configured password. If the password is forgotten, the unit must be sent back to 3Com support to have the feature disabled.

Configuration Scripting

The 3Com HomeConnect ADSL Modem Ethernet provides a scripting utility that will generate the CLI commands required to recreate a given configuration. After a unit has been configured as desired, the command:

```
show configuration script
```

will generate the list of CLI commands to the console.

The console output can be captured into a file on your workstation using the capabilities of your terminal emulation program or your TELNET utility. The captured file can then be altered as required and then "played" into the console of other unconfigured units.

As an alternative to directly executing a script file played into the console port, the 3Com HomeConnect ADSL Modem Ethernet is capable of executing a sequence of commands from a script file stored in FLASH memory. The file can be directly created in FLASH memory using the capture text command, or it can be created on a remote workstation and then transferred to FLASH memory using TFTP. To create the file using the CLI, use the command:

```
capture text <filename>
```

After invoking the command, anything you type at the console, anything you type at the console will be redirected to the specified file. To terminate input, type Ctrl-D. After the text has been captured, you can execute the commands at any time using the DO command as follows:

```
do <filename>
```

4 FILTERING CAPABILITIES

Introduction

The 3Com HomeConnect ADSL Modem Ethernet provides an extensive set of data filtering capabilities. For instance, filters can accept packets only from specific addresses to provide added security, or filters can be added to reduce network traffic and improve overall performance.

Packet filters control inter-network data transmission by accepting or rejecting the passage of specific packets through network interfaces based on packet header information. When data packets are received by a network interface such as an Ethernet (LAN) or WAN port, a packet filter analyzes the packet information using a set of rules you define. A filter then lets the packet pass through or discards it.

This chapter contains information on the filtering capabilities for your 3Com HomeConnect ADSL Modem Ethernet. It is divided into the following sections:

- Filtering Overview
- 3Com HomeConnect ADSL Modem Ethernet Filtering Capabilities
- Creating Filters
- Assigning Filters
- Applying Filters
- Managing Filters

Filtering Capabilities of the 3Com HomeConnect ADSL Modem Ethernet

The 3Com HomeConnect ADSL Modem Ethernet supports the following filtering capabilities:

- Input and output data filtering.
- Source and destination address filtering.
- Source and destination port filtering.
- Established session filtering. A packet filter can permit users to connect with a remote network without letting remote users have access to the local network (or vice versa).

Filter Classes

The 3Com HomeConnect ADSL Modem Ethernet supports the following filter classes:

- **Input data** - filter packets as they enter.
- **Output data** - filter packets as they exit.

Filter Types

Filters can be classified by the following types:

- **Data filters** - based on protocol-specific packet information.
- **Generic filters** - based on packet structure.

Data Filters

Data filters control network access based on the protocol and source / destination address of the packet.

Generic Filters

Generic filters are protocol-independent and are specified by byte and offset values in a packet. Packets are filtered by comparing each packet's offset value and byte information with the values that you define in the filter. The bridge will accept or reject the packet based on the result.

Creating generic filters can be a complex task. Only experienced users should employ generic filters, and strictly in cases where data and advertising filters cannot provide the filtering capabilities that you require.

Creating Filters

Before creating a filter file, you should carefully identify the information you want to filter. Decide if you want a filter that discards packets (such as reject all packets whose source MAC address is 002069000001) or accept only a subset of packets (such as accept only bridged packets if the destination MAC address is 002069000001 or 002069000002). Also determine where you want to place the filter. For example, figure out if you want to apply the filter to packets coming into the Ethernet interface, to packets going out the WAN (ATM) interface, or to packets coming from a specific port.

The first step in creating a filter on the 3Com HomeConnect ADSL Modem Ethernet is to create a file using filter syntax. The file can be created using a text editor on a remote workstation or it can be created using the CLI **create text** command. File names should be short and descriptive, such as BLOCKPC1.FLT.

The **create text** command simply redirects console input into a text file in the unit's FLASH memory. It does not provide any editing capabilities.

If you create the file on a remote workstation, you will need to transfer the file to the unit's FLASH memory using TFTP.

Once the filter file has been created and stored in the unit's FLASH memory, you then use CLI commands to add the filter to the list of filters and apply the filter to the appropriate interface or bridge port profile.

Filter File Components

You define the filtering rules used by the bridge within filter files. Filter files are text files that are stored in the unit's FLASH memory. You can create and modify filter files using an off-line text editor, then TFTPing the finished file on to the unit.

To be valid, a filter file must always have the following file descriptor on the first line: **#filter**

Be sure that no blank space precedes the descriptor, or an error will occur.

The file descriptor is followed by the bridge protocol section.

Protocol Sections/Bridge

The following conditions will generate errors or prevent normal filter operation:

- If you do not specify a protocol section in the filter file, no filtering will occur and packets of that protocol type will be accepted.
- If you specify a protocol section but do not define any rules, an error will occur.

To comment out the protocol section, you must place a pound (#) sign before the section header and before all rules defined in the section.

Protocol Rules

Protocol rules determine which packets may and may not access the network. The rule syntax is:

```
<line #> <verb> <keyword> <operator> <value>
```

The line # range is 1-998. This means you can combine up to 998 rules to create a filter for a specific protocol. Additionally, line number 999 is used for the DENY verb.

The combination of keyword, operator, and value forms the condition which (when combined with the verb) determines whether a packet is accepted or rejected.

When a packet is filtered, the bridge parses each rule defined in the protocol section sequentially according to the line number. Filtering is performed based on the first match that occurs. If there is no match, by default the packet is accepted. For this reason, you should order your protocol rules so that the rules you expect to be most frequently matched are in the beginning of the section. This reduces the amount of parsing time that occurs during filtering. The following table describes each field used in the rule syntax:

Table 4-1 Protocol Rules

Field	**Description**
line #	Each rule must have a unique line number from 1-998 plus 999 for the DENY verb. You must arrange rules in increasing order.
Verb	This field can be one of the following: **ACCEPT** - Allow the packet access if the condition is met (use with **DENY** verb to indicate reject all other packets). **REJECT** - Do not allow the packet access if the condition is met. **AND** - Logically use the AND condition with condition of the next rule to determine if the packet is accepted or rejected. Both defined conditions must be met.
Keyword	The keywords for all protocol, descriptions, corresponding operators and values.
Operator	Describes the relationship between the keyword and its value. The operator field must be one of the following: = Equal != Not equal > Greater than < Less than >= Greater or Equal <= Less or Equal => Generic
Value	Contains an entity that is appropriate for the keyword.

The OR operation can be implemented by successive rules. For example, to accept a packet if the source address is xxx, or the destination address is yyy, the following rules are used:

```
BR-ETH:
1 ACCEPT src-addr=00-20-69-00-00-01;
2 ACCEPT dst-addr=00-20-69-00-00-02;
999 DENY;
```

The following table describes the keywords for the bridge protocol section and their legal operators used in the rule syntax. (xx is a hex number).

Table 4-2 Protocol Keywords

ProtocolSection	Keyword	Operators	Description and Value Range
BR-ETH	src-addr dst-addr generic	=, != =, != =	Source MAC address (xx-xx-xx-xx-xx-xx) Destination MAC address (xx-xx-xx-xx-xx-xx) Generic filter

Generic Filter Rule

The syntax for generic filters is slightly different than that for other protocol filters:

```
<line #> <verb> GENERIC => ORIGIN = FRAME/OFFSET = <# of bytes>/
LENGTH = <# of bytes>/MASK = < 0x Mask>/VALUE = <0x value>
```

- **ORIGIN** - The location in the packet to start the offset count. This is at byte 0 (FRAME).
- **OFFSET** - The number of bytes from the origin to skip before comparing the value to the packet contents.
- **LENGTH** - The number of bytes in the packet to compare to the value.
- **MASK** - The mask to logically "and" with the packet contents before comparing with the value (hex).
- **VALUE** - The value (hex) to compare to the packet contents.

For example, a generic bridge filter to prevent all IP packets from being bridged is:

```
BR-ETH:
1 reject
generic=>origin=frame/offset=12/length=2/mask=0xFFFF/value=0x0800;
```

Step by Step Guide to Creating Filter Files

This section presents a step-by-step guide for creating and applying filters. These steps assume that the filter file is created on a remote workstation and then transferred to FLASH memory using TFTP. If you use the CLI create text command to create the filter file, you can omit steps 9 and 10.

To create a filter file:

1 Open a new text file. Enter the file descriptor on the first line: **#filter**

2 Enter the section header followed by a colon for the protocol rules you want to define. For example: **BR-ETH:**

3 You can comment a section header out by placing a # sign before the section header. This is useful if you want to insert a placeholder for a protocol section you

will define in the future. Also, use the # sign to add comments or what you expect the filter to do for future reference.

4 Enter the rules you are defining. Observe the following guidelines.

- Begin each rule with a unique line number ranging from 1 - 998.
- Arrange rules in increasing line number order within each protocol section.
- Arrange rules so that the rules you expect to be matched most frequently are toward the top of the list
- Delimit each rule with a semi-colon. Example:

```
BR-ETH 1 ACCEPT src-addr = 00-20-69-00-00-01;
2 ACCEPT src-addr = 00-20-69-00-00-02;
999 DENY;
```

5 Inspect the file to ensure that it meets all filtering rules.

6 This step is important since you cannot edit the filter file from within the CLI. To edit the file, you must modify it using a text editor, TFTP the modified file into the FLASH (replacing the original file) and verify the filter using the **verify filter** command.

7 Save the filter file using a **.flt** extension. The filter file extension will allow you to differentiate the filter file from other files stored in the bridge FLASH memory.

8 You can use the **list files** command to ensure the filter file was successfully stored in the bridge FLASH memory.

9 Configure a PC as a Trivial File Transfer Protocol (TFTP) client of the bridge by entering **add TFTP client <IP address>**.

10 From a machine that has access to the same network as the bridge, use a TFTP command to transfer the filter file to the bridge FLASH memory. For example, from the workstation command line enter **tftp <3Com HomeConnect ADSL Modem Ethernet IP address> put <filter filename>**

11 The bridge does not recognize a filter file stored in its FLASH memory until you add it to the managed filter table. To notify the unit about the filter file for the first time, you must issue the CLI command **add filter <name>** to add the filter to the managed filter table. When the filter is added, the unit automatically verifies the filter file syntax. If you modified a file that had already been added, use the **delete filter <name>** command to remove the old file before TFTPing the new file. Then use the **add filter <name>** command again or TFTP the new file over the old one and use the **verify filter <name>** command.

12 If the syntax is valid, no message is generated and the command prompt returns. If the syntax is not valid, error messages are generated detailing the source of the errors.

13 Apply the filter to the appropriate interface or port profile. After replacing a file, you need to re-apply the filter for the new filter file to take effect.

For more details, refer to the next two sections. **Assigning Filters** discusses how to decide where to apply a filter, and **Applying Filters** explains the appropriate CLI commands to use.

Assigning Filters

Once a filter has been added to bridge's list of managed filters, you can assign it to the unit's:

- Interfaces
- Ports

Interface Filters

You can configure interface filters for any interface. Interface filters control access to all networks available for both modem and non-modem interfaces. You can specify whether a filter applies to packets entering the interface (input filter) or leaving the interface (output filter). The bridge examines the filtering rules to determine whether the interface accepts or rejects the packet.

Input Filter

If an input filter is configured on an interface, all packets received into the bridge in that interface are checked against the filtering rules before being forwarded to another interface.

Output Filters

If an output filter is configured on an interface, all packets received into the bridge on that interface are checked against the filtering rules before exiting the bridge.

Input Filters vs. Output Filters

When possible, use the input filter to filter an incoming packet rather than waiting to catch a packet as it attempts to exit the bridge. This is recommended because:

- A packet is prevented from entering the bridge, keeping potential intruders from attacking the unit itself.
- The bridging engine does not waste time processing a packet that is going to be discarded anyway.
- Most importantly, the bridge does not know which interface an outgoing packet came in through. If a potential intruder forges a packet with a false source address (in order to appear as a trusted host or network), there is no way for an output filter to tell if that packet came in through the wrong interface. An input filter, on the other hand, can filter out packets purporting to be from networks that are actually connected to a different interface.

Port Filters

You can configure filters for a specific port profile that controls access to the network for that location. This filter is only applied for the duration of the remote network connection. As with interface filters, a port filter can be configured to apply to input or output data traffic.

Applying Filters

You can apply filters to interfaces and/or ports using the CLI. If you modify a file, you need to re-apply it to make the changes take effect immediately. Otherwise the changes will not take effect until the bridge network that the filter affects goes down and comes back up. This occurs when a network is disabled, the WAN connection goes down then up, or when the 3Com HomeConnect ADSL Modem Ethernet is rebooted.

Apply a Filter to an Interface

To configure an input or output filter on an interface, use the following CLI commands:

```
set interface <interface name> input_filter <filter name>
set interface <interface name> output_filter <filter name>
```

Interface name is **eth:1** for the Ethernet interface and **atm:1** for the ATM interface. For example, to apply an input filter to the ethernet interface:

```
set interface eth:1 input_filter filter.flt
```

*When assigning the filter to the Ethernet interface, you must turn off filter access by entering the CLI command **set interface eth:1 filter_access off.***

For more information about the filter access, refer to the **Setting Filter Access** section below.

Configuring a Filter for a Port

- To configure an input or output filter for a specific user, use the CLI commands:

  ```
  set port <port number>input_filter <filter_name>
  set port <port number>output_filter <filter_name>
  ```

- For example, to apply an output filter to port 2:

  ```
  set port 2 output_filter filter.flt
  ```

Setting Filter Access

When filters are assigned to both the WAN interface and a port profile, you need to tell the bridge which one to use using the filter access parameter. If filter access is ON, the port filters will override interface filters. If filter access is OFF, then the interface filters are used.

Always turn filter access OFF for the Ethernet interface since there are no profiles associated with it. If you do not turn if off, the filter will not be applied.

- To set the filter access parameter to ON for a specific interface, use the CLI command:

  ```
  set interface <interface_name> filter_access ON
  ```

- To set the filter access parameter to OFF for a specific interface, use the CLI command:

  ```
  set interface <interface_name> filter_access OFF
  ```

Managing Filters

This section provides information about how to perform filter management tasks.

Displaying the Managed Filter List

- To display the list of managed filters, use the following command:

  ```
  list filters <filter_name>
  ```

The resulting display might look like this:

```
Filter Name       Status         Protocols
 filter.flt       NORMAL          BR-ETH
```

Adding Filters to the Managed List

The **add filter** command verifies filter syntax prior to adding the filter to the managed list. If the syntax is valid, no message is generated and the command prompt returns. If syntax errors exist, error messages are generated detailing the cause of the errors.

If the syntax is invalid, the filter is still added to the managed list with a status of verify failed. To correct filter file errors, you must make the changes to the original filter file using a text editor, and re-TFTP the file to the bridge's FLASH memory.

Then use the **verify filter** command to check the filter file syntax.

- To add a filter file to the list of managed filters, use the CLI command

```
add filter <filter name>
```

It may be helpful to use the **list files** command to see files successfully stored in the FLASH memory.

Removing a Filter from an Interface

- To remove a filter that is assigned to an interface, use the following command:

```
set interface <interface name> input_filter ""
set interface <interface name> output_filter ""
```

The " " value represents a null value and removes the defined filter from the interface. For example, to remove an output filter from an interface named eth:1, you would use the following command: **set interface eth:1 output_filter ""**

Removing a Filter from a Port Profile

- To remove a filter that is assigned to a port profile, use the following command:

```
set port <port number> input_filter ""
set port <port number> output_filter ""
```

The " " value represents a null value and removes the defined filter from the user profile.

- For example, to remove an input filter from port #2, you would use the CLI command:

```
set port 2 input_filter ""
```

Deleting a Packet Filter

- To delete a specific packet filter, removing the filter file permanently from the FLASH memory, use the CLI command

```
delete filter <filter_name>
```

Verifying Filter File Syntax

The verify filter command must be used if you make changes to a filter file that has already been added to the managed list and re-TFTP it back to the bridge's FLASH memory (using the same filename). The verify filter file will check the filter syntax. If the syntax is valid, no message is generated and the command prompt returns. If the syntax is not valid, error messages are generated detailing the source of the errors.

- To verify a filter file, use the CLI command

```
verify filter <filter_name>
```

Showing Filter File Contents

- To view the contents of an entire filter file that has been added to the managed list of filters, use this command:

```
show filter <filter_name>
```

5 UPGRADING 3COM HOMECONNECT ADSL MODEM ETHERNET OPERATIONAL SOFTWARE

Introduction

The 3Com HomeConnect ADSL Modem Ethernet operational software is stored in the unit's FLASH memory. There are two ways to update the operational software:

- You can load new software through the serial console port.
- You can load new software using the unit's built-in FTP or TFTP client software.

Serial Port Update

For serial port updating, there are three methods of obtaining the latest versions of the 3Com HomeConnect ADSL Modem Ethernet Operational Software. Choose the method that best suits you.

- 3Com Instant Update Process - This is the preferred method of obtaining the operational software and documentation. Use the 3Com Instant Update to check for the latest available version of the software, then download the software.
- 3Com FTP Site - Access the 3Com FTP Site to obtain software and documentation
- 3Com HomeConnect ADSL Modem Ethernet CD - Install from the CD if you have the latest version of the software on CD.

If you have erased the operational software from your 3Com HomeConnect ADSL Modem Ethernet, you will need to reinstall the software from your CD.

3Com Instant Update Process

If you have not yet installed Instant Update and configured it, you will need to do so. The 3Com Instant Update is included on the 3Com HomeConnect ADSL Modem Ethernet CD.

Open the **Scheduling** tab on the Instant Update Screen. Click **Update Now**. Instant Update will prompt you to continue, and after you agree to this, it will copy the new 3Com HomeConnect ADSL Modem Ethernet software to your hard drive (to the default path of **c:\Program Files\3Com\3Com HomeConnect ADSL Modem Ethernet\Update**).

You are now ready to install the 3Com HomeConnect ADSL Modem Ethernet operational software to the unit. Continue to the **Install Software via DOS** section.

3Com FTP Site

It is possible to obtain the latest 3Com HomeConnect ADSL Modem Ethernet operational software from the 3Com FTP site, without installing or running the 3Com Instant Update.

Launch your browser and enter in the location of the 3Com FTP site **ftp.3com.com** in your browser's address or location field. You will then need to navigate through the directory structure to **pub/xdsl/hceth**. From this site, you can obtain document updates from the DOCS subdirectory and code updates from the BINARIES subdirectory.

The code updates are stored in two forms in the BINARIES subdirectory. One form is a self-extracting executable (with the extension .EXE) that contains the new operational software along with the supplemental utilities required to load the software into the unit via the serial port. The filename reflects the version of the code (i.e., V010109.EXE would contain version 1.0.9).

The second form is simply the operational software itself. This can be used with the Built-in Update procedure presented later in this chapter which directly loads the software into the modem without storing the code on a PC. Files containing the operational software only have the .NAC extension.

For serial port update, select the appropriate EXE file from the BINARIES directory and store it to an empty subdirectory on your PC. You should execute the self-extracting EXE to unzip the files to the local subdirectory. Continue to the **Installing Operational Software via DOS** section.

3Com HomeConnect ADSL Modem Ethernet CD

If you have obtained an updated 3Com HomeConnect ADSL Modem CD, or if you have erased the copy of the 3Com HomeConnect ADSL Modem Ethernet Operational Software from your hard drive, you need to copy the operational software from the CD to your hard drive.

1. Insert the 3Com HomeConnect ADSL Modem Ethernet Installation CD in your PC's CD drive (for example, drive **d:**). An installation menu will be displayed.
2. Click **Install the HomeConnect ADSL Modem Ethernet**.
3. Follow the prompts on your screen to finish the software installation. In addition to installing the 3Com HomeConnect ADSL Modem Ethernet operational software, this will also install the utilities and printable documentation.

The 3Com HomeConnect ADSL Modem Ethernet operational software (the *.nac file) included on the CD is copied to your hard drive and not the 3Com HomeConnect ADSL Modem Ethernet unit. It is installed to **c:\Program Files\3Com\3Com HomeConnect ADSL Modem Ethernet\Update**.

Installing Operational Software via DOS

Your 3Com HomeConnect ADSL Modem Ethernet Installation CD installs a DOS-based utility program onto your hard drive. This utility program, PCSDL.EXE, is invoked by a DOS-batch file, DL.BAT, which has also been installed to your drive.

In order to use PCSDL to load code to your 3Com HomeConnect ADSL Modem Ethernet, use the console port straight-through console cable (provided) between your workstation's serial port and the unit's console port.

To update the software from DOS, perform the following:

1. Using a terminal application such as HyperTerminal to test the serial connection, set up the terminal application with the following settings:
   9600 baud, No stop bits, 8-bit characters, no parity
2. Press **Enter** on your workstation. If the terminal application displays the '3com homeconnect adsl modem ethernet>' prompt, the serial connection is operational. You should now close the terminal application (Hyperterminal).

3 Power off your 3Com HomeConnect ADSL Modem Ethernet.

4 Open a DOS window on your workstation.

5 Change to the directory containing the new operational software. If you obtained the software from the Installation CD or using Instant Update the default directory is **c:\Program Files\3Com\3Com HomeConnect ADSL Modem Ethernet\Update**.

The DL.BAT batch file uses the Com 1 port by default. You can change the port used by editing the DL.BAT file. The relevant lines of the file are shown below.

```
REM
REM Edit the pcsdl command line -v parameter so that it includes
REM the REM version number of the NAC file. The version number of
REM the NAC file is part of the filename. The filename syntax is:
REM
REM      mdxxyyzzc where xx = major version number
REM                     yy = minor version number
REM                     zz = revision number
REM
REM Release 1.0.4 would have a filename of md010004.
REM
REM
REM Change the -p option on the pcsdl command line to use the
REM proper COM port.
pcsdl -p1 -r%BAUDRATE% -vNA1.0.4 -vSD0.3.3 -nSDmd -nNAmd

pcsdl -p1 -r%BAUDRATE% -vNA1.0.4 -vSD0.3.3 -nSDmd -nNA
```

Execute the batch file with the following command:

- **dl 115**

6 When `Establishing Communications...` appears in your DOS window, plug the 3Com HomeConnect ADSL Modem Ethernet back into the outlet.

7 Various status messages will be displayed, indicating the progress of the download. The download should take approximately 3 minutes to complete.

Update Using Built-in Update Software

The **update software FTP** and **update software TFTP** commands allow you to utilize the 3Com HomeConnect ADSL Modem Ethernet FTP or TFTP clients to obtain and install the new operational software. You can access these commands directly from the serial console CLI session or through TELNET.

The 3Com HomeConnect ADSL Modem Ethernet must have an IP address configured in order to use the built-in update commands. See the **IP Configuration** section of Chapter 3 for information on configuring IP.

To update the software using the FTP command, use the CLI command:

update software ftp <filename>

- **server <ip_addr or host_name>**
- **path <path>**

- **username <username>**
- **password <password>**

If you are obtaining the code update from the 3Com FTP site, you would use the command:

update software ftp <filename>

- server **ftp.3com.com**
- path **/pub/xdsl/hceth/binary**
- username **anonymous**
- password **<password>**

where <filename> is the NAC file to load and <password> is your email address (i.e., name@company.com). See the previous section **3Com FTP Site** for more information about files available from the 3COM FTP site.

To update the software using the TFTP command, use the CLI command:

update software tftp <filename>

- **server <ip_addr>**
- **path <path>**

A CLI COMMAND DESCRIPTION

CLI Commands

ADD

Use the ADD command to define:

- networks you will connect to
- SNMP communities
- users who can telnet to the unit

Note that some parameters have default values.

add bridge access_mac_address <mac_address>

Adds a MAC Address to the Access MAC table. When the Access MAC feature is enabled, only MAC Addresses in the Access MAC Table will be bridged.

Parameters	Description
<mac_address >	The MAC address being granted access.

add dns server <domain_name>

primary_address [ip_address]

secondary_address [ip_address]

Adds the IP Address of a remote DNS Server for the specified Domain Name to the Domain Name Server Table. The IP Host Name is first sent to the Primary Server to be resolved. If that server cannot resolve the name, a request is sent to the Secondary Server.

Parameters	Description
<domain_name>	Domain name. Use * for all domains.
primary_address	The primary IP address of the DNS server.
secondary_address	The secondary IP address of the DNS server.

add filter <filter name>

Parameters	Description
<mac_address >	The MAC address being granted access.

Adds a filter file name to the filter table. The filter table is a managed list of filter names used by SNMP. A filter file is a text file stored in the FLASH file system, that you load using TFTP. *Add filter* also verifies the syntax of the filter file. If syntax verification fails, you'll receive an error message, and the filter will still be added to the table, but is not usable. You must correct the filter file in a text editor, use

TFTP to export the updated file to the system's FLASH file system, and use the *verify filter* command to check the filter's syntax.

Parameters	Description
<filter_name>	Designation of a filter file, up to twenty ASCII characters.

add ip defaultroute gateway <IP_address>

{ metric [1] }

Defines a default gateway IP router, which acts as the default route for IP packets destined for remote hosts.

Parameters	Description
<IP_address >	IP Address of the gateway router.
metric	Integer representing how far away the default router is, in "hops" through other routers. Values: 1-15.

add ip network <network_name>

address [ip_net_address]
frame [ETHERNET_II | SNAP | LOOPBACK]
{ interface [eth:1] }
{ enabled [yes] }

Adds an IP network to the list of IP networks available over the specified interface.

Parameters	Description
<network_name>	Name of IP network, consisting of up to 32 unique ASCII characters; space must be surrounded by double quotes.
address	IP address of the network, in the format nnn.nnn.nnn.nnn, with or without a mask specifier. The Mask Specifier can be 'A', 'B', 'C', or 'H', or a numeric value from 8 to 30 that describes the number of one bits in the mask. If you do not specify a mask, the system will gener ate it for you from the network address.
frame	Frame encapsulation to be used on this IP network. The options are: ETHERNET_II, LOOPBACK (for diagnostics), or SNAP.
interface	Name of the interface which this IP network will communicate over. The default is the first LAN interface (eth:1).
enabled	This optional parameter indicates whether the network is enabled (YES) or disabled (NO). YES is the default.

add ip route <ip_net_address>

gateway [gateway_addr]

metric [hop_count]

Adds an entry to the IP routing table. IP packets destined for networks that match this network will be routed to this address. The command *list ip routes* displays your currently defined routes.

Parameters	Description
<net_address>	IP address of the remote network, in the format nnn.nnn.nnn.nnn, with or without a mask specifier. The Mask Specifier can be 'A', 'B', 'C', or 'H', or a numeric value from 8 to 30 that describes the number of one bits in the mask. If you do not specify a mask, the system will generate it from the network address.
gateway	IP address of gateway used to reach this remote network.
metric	An integer representing how far away the route is, in "hops" through other routers. Values are 1-15.

add snmp community <community_name>

address [IP_address]

access [RO | RW]

Adds to the list of SNMP authorized users. The community name and IP address of SNMP requests from managers on the network must match the list, which you can see using *list snmp communities*.

Parameters	Description
<community_name>	Group name that authorizes SNMP requests.
address	IP address of the SNMP manager, in the form nnn.nnn.nnn.nnn
access	Determines what type of access to SNMP MIBs the added user will have. Options: Read Only (RO) and Read Write (RW).

add snmp trap_community <name>

address <IP_address>

Adds to the list of community name/IP address pairs that are allowed to receive SNMP traps. You can see the list of authorized users with the *list snmp communities* command.

Parameters	Description
<name>	Group name defining who can receive SNMP traps.
address	IP address of the SNMP manager, in the form nnn.nnn.nnn.nnn

add syslog <ip_addr> loglevel [loglevel]

Adds an IP host to the list of IP hosts that will receive syslog entries. You can see the current log levels for the system using *list facilities*, and modify the current log level for each facility using *set facility loglevel*.

Parameters	Description
<ip_address>	IP address of the Unix host that will receive sys log information.
loglevel	There are five levels of logging: **CRITICAL** - a serious system error, which may effect sys tem integrity **UNUSUAL** - an abnormal event, which the system should be able to recover from **COMMON** - a regularly occurring event that is not frequent **VERBOSE** - a regular periodic event, e.g. a routing update message **DEBUG** - for debugging only

add tftp client <ip_addr>

Adds the tftp client to the authorization table for tftp access.

Parameters	Description
<ip_addr>	IP address of a host to be added. An address of 0.0.0.0 allows all clients TFTP access.

add user [name] password [password]

{enabled [yes]}

Adds a Telnet user to the local user table. The *list users* command displays these parameters for all users.

Parameters	Description

Name	Name of the user to be added, up to 32 ASCII characters.
Password	User's password, up to 15 ASCII characters.
Enabled	This indicates whether the user is enabled. Enter **YES** or **NO**.

CAPTURE TEXT

capture text <filename>

Redirects console input into a text file. Input redirection is terminated by Ctrl-D. This command serves as a simple way to create filter files or to create command scripts that can be executed using the **DO** command.

DELETE

Delete commands remove anything you previously *add*ed.

delete bridge access_mac_address <mac_address>

Deletes a MAC Address to the Access MAC table. When the Access MAC feature is enabled, only MAC Addresses in the Access MAC Table will be bridged.

Parameters	**Description**
<mac_address >	The MAC address being denied access.

delete configuration

Deletes all your configuration files, reboots the system and restores system configuration to default values.

delete dns server <domain_name>

Removes the name server addresses associated with the specified domain from the Domain Name Server Table.

delete file <file_name>

Deletes a file from the FLASH file system. Use *list files* to see which files are currently stored.

delete filter <filter_name>

Removes the named filter from the filter table, and deletes the file stored in FLASH memory. Use *list filters* to see what filter files are in FLASH memory.

delete ip network <network_name>

Deletes an IP network from the interface that you specified when *add*ing the network. Use *list ip networks* to see which networks are associated with which interfaces. Always use *disable ip network* before deleting it.

delete ip route <IP_address>

Deletes an IP address from the IP routing table, that you previously added with *add ip route*. Deleting this route will cause IP packets destined for this network to use the default route, which you can see using *list ip routes*. See *add defaultroute gateway* to find out how to add a default route.

delete snmp community <name>

Deletes an SNMP community that was previously added with the *add snmp community* command. You can use *list snmp communities* to see the current entries.

delete snmp trap_community <name>

Deletes an SNMP trap community name from the list of names and IP addresses that are allowed to receive SNMP trap commands. You can use *list snmp communities* to see the current entries.

delete syslog <ip_addr> Deletes the specified IP address from the list of addresses which are authorized to receive syslog information. Use *list syslog* to see the currently allowed addresses.

delete tftp client <ip_addr> Deletes the specified IP address from the list of addresses which are authorized to TFTP. Use *list tftp clients* to see the currently allowed addresses.

delete user <name> Deletes a user you previously added to the local user table. Use *list users* to see the currently defined user, and *show user* to see the attributes you assigned to that user using the *add user* or *set user* command.

DISABLE

disable bridge access_mac_addresses Disables the Access MAC feature. When the Access MAC feature is enabled, only MAC Addresses in the Access MAC Table will be bridged.

disable bridge forwarding Globally disables bridging.

disable bridge spanning_tree Disables use of the spanning tree. The spanning tree algorithm is required if there is more than one bridge between the same two LAN segments.

disable ip network <network_name> Disables the specified IP network. Make sure there is no activity on this network before disabling it.

disable link_traps interface <interface_name> Prevents SNMP from sending linkup and linkdown traps for the specified interface. You can see if the interface is currently enabled for traps by using the *show interface settings* command.

disable port <port number> Disables the specified bridge port from being used.

disable security_option snmp user_access Turns off SNMP access to the CLI. This prevents remote users from using SNMP and possibly damage the configuration. You can use *enable security_option snmp user_access* to re-enable full SNMP access.

disable security_option remote_user administration Disables CLI access to remote TELNET users. All CLI configuration must be done from the console port. You can use *enable security_option remote_user administration* to re-enable remote CLI access.

disable snmp authentication traps Instructs SNMP to not generate a trap when an access is made using an unknown community.

disable user <user_name> Disables the specified user from being used. It also causes all active sessions established using that particular user to terminate, and does not allow any new sessions to occur using that user name. Disabling a user is useful when prohibiting a user’s access temporarily.

DO

do <command_inputfile> output [outputfile]

Runs a script file that is stored in FLASH memory, which contains a series of CLI commands.

ENABLE

enable bridge access_mac_addresses

Enables the Access MAC feature. When the Access MAC feature is enabled, only MAC Addresses in the Access MAC Table will be bridged.

enable bridge forwarding

Globally enables bridging.

enable bridge spanning_tree

Enables the spanning tree algorithm for the bridge connection. The spanning tree algorithm is required if there is more than one bridge between the same two LAN segments.

enable ip network <network_name>

Enables the specified IP network, which you previously defined using *add ip network*. You can use *list ip networks* to see the currently defined IP networks, as well as their current status.

enable link_traps interface <interface_name>

This command tells SNMP to send linkup and linkdown traps for the specified interface. You can see if the interface is currently enabled for traps using the *show interface settings* command.

enable port <port number>

Enables a bridge WAN port. The *list port* command displays a summary of all bridge ports.

enable security_option remote_user administration

Enables CLI access via TELNET. You can use *disable security_option remote_user administration* to restrict CLI access to the console port only and *enable security_option remote_user administration* to re-open full TELNET access.

enable security_option snmp user_access

Enables SNMP access to the user table. This allows remote users to use SNMP to update the user table, and gain unauthorized access to the CLI. Use *show security_options* to see the current security values.

enable snmp authentication traps

This command tells SNMP to send a trap when access is made using an unknown community.

enable user <user name>

Enables a TELNET profile. You must have previously added the profile using the *add user* command. The *list users* command displays a summary of all configured TELNET profiles.

exit CLI

If CLI password protection is enabled, this command forces an immediate logout from the CLI. The CLI password must be entered in order to access the CLI again.

HELP

help <command> Provides information about possible commands and their formats. Typing help alone lists the possible commands. Typing help <command name> lists the possible parameters for that command.

Typing part of a keyword (command or parameter) and pressing Esc completes the keyword. If you have not yet entered enough of the keyword to be unique, pressing Esc causes the bell to ring.

Typing **?** after a command string displays the possible keywords and values for that command.

HISTORY

history Displays your previous CLI commands. You can recall commands from the history using ^P (C-P) to recall commands up the list, and ^N (C-N) to recall commands working down the list. The default depth is 10 commands. You can modify the history depth using the *set command history* command.

idle timout <minutes> Sets the CLI inactivity timeout period. If the CLI is idle for the idle timeout period, and if CLI password protection is enabled, the CLI password must be re-entered before any commands can be executed.

LIST

list bridge access_mac_addresses Lists the contents of the the Access MAC Table. When the Access MAC feature is enabled, only MAC Addresses in the Access MAC Table will be bridged.

list bridge forwarding Displays the forwarding and filtering information

MAC address - A unicast MAC address for which the bridge has forwarding and/or filtering data

Status - One of:

other - not one of the following

invalid - aged out

learned - learned, and in use

self - statically defined, and in use

mgmt - unknown, but filtering information exists

RxPkt - Number of packets received from this MAC station

RxOctets - No. of bytes (octets) received from this MAC station

Fltr - Number of packets received from this MAC station that were filtered out (discarded)

Fwd - Number of packets received from this MAC station that were forwarded

TxPkt - Number of packets forwarded to this MAC station

TxOctets - Number of bytes forwarded to this MAC station

list connection events Displays the contents of the Connection Event Table. This table displays informational and error messages regarding the establishment of wide are connections.

list dns servers Displays DNS Name Servers, which you configured using the *add dns server* command. The domain name and the server address are listed for each DNS server.

list facilities Displays the system facilities (processes) currently running, plus the default log level. The log level is the severity of error that facility will produce syslog entries for. You can change the log level using the *set facility loglevel* command.

list filters Displays all the filter names in the filter table, which you previously defined using the *add filter* command. You can remove filters using *delete filter*. The command lists the filter file name, the status of the filter, and the protocols the file applies to. For example:

```
Filter Name         Status Protocols
easyfilter.fil      NORMALBR BR-ETH
```

list files Displays the files currently stored in the FLASH file system. You can remove files using *delete file*, but you can add them using TFTP only.

list interfaces Displays the installed interfaces, along with their operational status, administration status, and interface index. If an interface is down, you can use *enable interface* to try to bring it up. The command lists:

- Index - number used to identify the interfaces position in the table
- Name - interface name: eth:1 or atm:1
- Oper Status - current, operating status of interface; UP or DOWN
- Admin Status - administrative status you designated interface to be, up or down. If it doesn't match Oper Status, a problem exists with the interface.

list ip addresses Displays the IP address for each interface. It lists:

- **Address** - IP address of the interface
- **Bcast Algo** - broadcast algorithm used
- **Reassembly Max Size** - maximum allowable size of packet that can be reassembled from a fragmented packet

- **Interface** - interface this IP address uses to connect to the system

list ip arp Displays the contents of the ARP cache. It lists:

- **IP Address** - IP address for this entry
- **Phys Address** - MAC address that the IP address maps to
- **Type** - interface type: Ethernet or Token Ring
- **If Name** - *eth:1, DA:1* or *loopback*

list ip networks Displays all the IP networks you previously defined using the *add ip network* command. It also lists:

- **Name** - network designation
- **Prot** - always the IP protocol
- **Int** - name of the interface this network runs on
- **State** - state of the network; ENABLED or DISABLED
- **Type** - STATIC or DYNAMIC network
- **Network Address** - address of the IP network

list ip routes Displays all the statically defined IP routes that you previously defined using the *add ip route command*. It lists:

- **Destination** - IP address that the route resolves to
- **Prot** - LOCAL
- **NextHop** - address of the gateway used to reach this route
- **Metric** - number of router hops away this route is from the system
- **If** - interface that the route uses

list ports Lists all bridge ports, showing:

- **Name** - user designation you specified using *add vc*
- **Network Service** - type of network service: e.g., RFC1483
- **VPI** - Virtual Path Identifier
- **VCI** - Virtual Channel Identifier
- **Status** - link status: ACTIVE, INACTIVE or DISABLED

list snmp communities or list snmp trap_communities These commands display the defined SNMP communities, which you previously defined using the *add snmp community* command. *SNMP trap_communities* does not list access.

- **Community Name** - community designation for the IP address
- **IP address** - IP address of a member of the community
- **Access (Read/Write)** - type of access a member has to MIBs

list syslog

Displays IP addresses which get syslog entries from the system. See *add syslog* for more information, and *delete syslog* command to remove entries. This command shows:

- **Syslog** - IP address to which syslog entries will be sent
- **Log Level** - reporting level of entries to send
- **Msg Count** - current number of messages sent since system bootup

Also see *list facilities* and *set facilities* commands, which let you view and change log reporting levels for each system facility.

list tftp clients

Displays IP addresses of all users who allowed to use the Trivial File Transfer Protocol (TFTP) to connect to the system. You must have used *add network service* to add TFTP support to the system and used *add tftp client* to authorize users to connect.

list users

Lists all users, showing:

- **User Name** - user designation you specified using *add user*
- **Login Service** - The service used to login to the network (i.e. TELNET).
- **Status** - link status: ACTIVE, INACTIVE or DISABLED

PAUSED COMMANDS

More (or CR)	Continue printing
Quit	Cancel rest of output

PING

ping <ip_name_or_addr>

output [output_filename]

count [count]

interval [interval]

timeout [timeout_value]

Sends an ICMP echo request to a remote IP host. A reply from the pinged address indicates success.

Parameters	Description
<ip_name_or_address>	IP address in dotted notation, or host name of remote system.
output	A file name to direct output to.
count	Number of ICMP echo requests to send.
interval	Number of seconds to wait between sending each request.
timeout	Number of seconds to wait for an echo response to return.

REBOOT

Reboot the system. If you have made any configuration changes, be sure to *save all* before rebooting. Also see the *delete configuration* command.

RENAME

rename file <input_file> <output_file>

Renames files within the FLASH file system. The FLASH file system is a flat file system (no subdirectories). Use the *list files* command to see what files currently exist.

Parameters	Description
<input_file>	Name of the original file.
<output_file>	New name for the file

reset ethernet counters

Clears the statistics counters for the Ethernet port.

reset port <port number> **counters**

Clears the statistics counters for the specified bridge port.

SAVE

save all

Saves all changes you have made during your session with the CLI. It is a good idea to save your changes frequently, just as you should with any type of editor.

SET

set adsl option <optn_value>

Allows the setting of the ADI OPTN CMV. In order for the change to take effect, you must reset the ADSL chipset using the *set adsl reset* command.

set adsl power hi

Sets the maximum power spectral density (PSD) value used by the Analog Devices 918 ADSL chipset to the recommended non-restricted value. This can be used to get increased performance when connecting to newer ADI 918-based DSLAMS. Use the **show adsl config** command to display the currently configured value. The new PSD value takes effect on the next ADSL line retrain. To force a line retrain, use the **set adsl reset** command.

set adsl power lo

Sets the maximum power spectral density (PSD) value used by the Analog Devices 918 ADSL chipset to the recommended restricted value. This is the recommended setting when connecting to older ADI 910-based DSLAMs. This is the default setting. Use the **show adsl config** command to display the currently configured value. The new PSD value takes effect on the next ADSL line retrain. To force a line retrain, use the **set adsl reset** command.

set adsl psdm <psdm_value>

Sets the maximum power spectral density (PSD) used by the Analog Devices 918 ADSL chipset. This command can be used to restrict the output power. Use the **show adsl config** command to display the currently configured value. The new PSD value takes effect on the next ADSL line retrain. To force a line retrain, use the **set adsl reset** command.

set adsl reset

Resets the ADSL interface.

set bridge **aging_time <seconds>**

forward_delay <seconds>

spanning_tree_priority <seconds>

Sets parameters for all bridge networks.

Parameters	Description
aging_time	Interval to wait before aging out MAC addresses that were learned from other LAN segments. The default is 300.
forward_delay	Interval bridge waits before bridging packets. This time is useful for the bridge to listen to packets, look at the MAC addresses, and build its known MAC address table. Default is 15 seconds.
spanning_tree_ priority	Priority number determines who will be seen as the “root” bridge in a bridge network. The default is 32768.

set command **history <numerical range>**

idle timout <minutes>

local_prompt <string>

prompt <string>

login_required Enables or disables CLI password protection.

password The CLI password. It must consist of 1 to 8 alphanumeric (printable) characters, inclusive.

Sets console parameters for CLI commands.

Parameters	Description
history <numerical range>	Sets the depth of the buffer holding the command history. Use the *history* command to see the current depth and a list of your last CLI commands. The default is 10 commands. Range: 1-500.
prompt **<**string**>**	**Sets the global command prompt for the CLI. Use** *show com mand* to see the currently defined prompt. Limit: 64 characters.
local_prompt <string>	Sets a separate prompt for a command file process. Limit: 64 characters.
login_required [YES | NO]	Set to YES if CLI console passwording is enabled.
password <alphanumeric string>	The CLI password, up to 8 characters

set date <date> Sets the system date, and leaves the time unchanged. Use *show date* to see what the current settings are. The format is: dd-mmm-yyyy. The month should be the first three characters of the month name. The year can be either 2 or 4 digits - 99 or 1999.

set facility <facility_name> loglevel [level] Sets the severity reporting level for a facility. The hosts that will receive the error log entries are defined using *add syslog loglevel*. Use *list facilities* to see what the current loglevel is for each facility. The levels:

- **CRITICAL** - a serious system error, which may effect system integrity

- **UNUSUAL** - an abnormal event, which the system should recover from
- **COMMON** - a regularly occurring event that is not frequent
- **VERBOSE** - a regular periodic event, e.g. a routing update message
- **DEBUG** - for debugging purposes only

set interface <interface_name>

filter_access [ON | OFF]

input_filter <filter_name>

output_filter <filter_name>

Sets filter parameters for the specified protocol on the specified interface. You can see the available filter files using *list filters*, view the contents of a filter file using *show filter*, and add filter files to FLASH memory using TFTP.

Parameters	Description
<interface_name>	Designation of interface you are setting parameters for. Limit of 32 characters.
filter_access	ON causes filters specified for an interface with a *set interface* com mand, to override filters specified with a *set user* command, when the filters are of the same type.
input_filter	Name of filter file you wish to be applied to the input stream coming in on the specified interface. Limit: 20 characters.
output_filter	Name of the filter file you wish to be applied to the output stream leaving the specified interface. Limit: 20 characters.

set port <port number>

pcr [number]

vci [number]

vpi [number]

description [filter_name]

input_filter [filter_name]

output_filter [filter_name]

Specifies bridge port parameters.

Parameters	Description
<port number>	Port number (2..9)
input_filter	Designation of the filter file in FLASH memory to be applied to the input data stream.
output_filter	Name of the filter file in FLASH memory to be applied to the out put data stream.
Pcr	Peak Cell Rate (both UBR and VBR).
Vci	Virtual Channel Identifier.
Vpi	Virtual Path Identifier.

set snmp community <community_name>

address [IP_address]

access [RO | RW]

Modifies parameters for an SNMP authorized user. The community name and IP address of SNMP requests from managers on the network must match the list, which you can see using *list snmp communities*.

Parameters	Description
<community_name>	Group designation authorizing SNMP requests.
address	IP address of the SNMP manager, in the form nnn.nnn.nnn.nnn
access	Determines what type of access to SNMP MIBs the added user will have. Options are Read Only (RO) and Read Write (RW).

set snmp trap_community <name>

address <IP_address>

Changes the IP address pairs that are allowed to receive SNMP traps. You can see the list of authorized trap communities and addreses with the *list snmp trap_communities* command.

Parameters	Description
<name>	Group name defining who can receive SNMP traps.
address	IP address of the SNMP manager, in the form nnn.nnn.nnn.nnn

set system

name [“name”]

location [“location”]

contact [“contact info”]

Specifies system contact information, which is displayed using *show system*. The user name is the remote account name. *Location*, *name* and *contact* names are limited to 64 characters..

Parameters	Description
name	A name identifying the user to the system.
location	The location of the user.
contact	The information contact for the user.

set syslog <IP_address> loglevel [level]

Sets the error reporting level for syslog entries that will be sent to the specified IP address. You must have previously defined this syslog IP address using *add syslog*.

There are five levels of logging:

- **CRITICAL** - a serious system error, which may effect system integrity
- **UNUSUAL** - an abnormal event, which the system should recover from
- **COMMON** - a regularly occurring event that is not frequent
- **VERBOSE** - a regular periodic event, e.g. a routing update message
- **DEBUG** - for debugging only

set time <time>

Sets the system time, and leaves the date unchanged. Use *show date* to see what the current settings are. The format is: hh:mm:ss. The seconds field is optional.

set user <user_name>

message [“message”]

password [password]

session_timeout [seconds]

tcp_port [tcp_port]

terminal_type

Modifies user parameters.

Parameters	**Description**
<user_name>	Name of user, previously defined using *add user*. Limit of 32 char acters.
message	Message presented to a dial-in user.
password	User’s password, up to 15 ASCII characters. Value is required.
session_timeout	Interval before timing out a session.
tcp_port	TCP Port number for the Telnet session.
Terminal_type	The type of the terminal. This is an alphanumeric string, of up to 64 characters.

SHOW

Show commands display details about system entities.

show adsl configuration

Displays the current status of the command-line configurable ADSL chipset items.

- Option register - the OPTN CMV value to on the next reset of the ADI chipset.
- PSDM config register - the ADSL maximum power spectral density setting.

show adsl performance

Displays ADSL error statistics. The following statistics and counters are collected in 15-minute interval bins:

- Loss of framing errors
- Loss of power errors
- Errored seconds
- Loss of signal errors

The statistics are displayed for the following time periods:

- Current 15-minute interval
- Previous 15-minute interval
- Current day
- Previous day
- Total

show adsl statistics

Displays block count statistics for the ADSL interface. It reports the number of blocks transmitted and received. It also reports the number of blocks received with corrected errors, and the number received with uncorrectable errors.

show adsl transceiver_status

Displays the current status of the ADSL transceiver. It lists:

- **Operational Mode –** Current operational mode of the transceiver.
- **Attenuation** – the difference in dB between transmitted and received signal power.
- **Signal to Noise Ratio Margin** – the SNR margin required by the transceiver to maintain the ADSL link.
- **Transmit Power** - The transmit power in dB of the local ADSL transceiver.
- **Code Word Length** – The current code word size for the fast interlayed paths.
- **Downstream Rate** – the negotiated bit rate for data received from the network.
- **Upstream Rate** – the negotiated bit rate for data transmitted to the network.

show adsl version

Displays version information about the ADSL interface. It lists:

- **Hardware Release Version** - Version of the ADSL chipset present on the unit.
- **Firmware Release Version** - Version of the ADSL firmware present on the unit.

show atm status

Displays current statistics for the ATM protocol running over the ADSL WAN interface. It lists:

- **Cell Delineation** - Whether or not cell delineation is currently achieved.
- **RX No Pkt Avail** - Number of times a packet was reassembled but could not be delivered over the LAN because of lack of packet memory within the HomeConnect ADSL Modem.
- **RX Bad VPI or VCI** - Number of ATM cells received with a bad or inactive VPI and/or VCI number.

show bridge settings

Displays the settings for all bridge networks. Use *set bridge* to modify these values.

- **Base Aging Time** - time to age out a known MAC address, default 300
- **Spanning Tree Forward Delay** - delay after coming up before learning, default is 15
- **Spanning Tree Priority** - this bridge's bid to be root bridge, default is 32768
- **Access MACs Only** - This can be enabled or disabled.
- **Spanning Tree Mode** - sets spanning tree algorithm on. Default is DISABLED
- **Base MAC Address** - address of the bridge
- **Number of Networks** - number of networks in this bridge

show command

- Displays the settings for Command History Depth, and the Current Prompt. You can modify the history depth using *set command history*, and alter the prompt using *set command prompt*. Prompts can hold a maximum of 64 characters. For example:

```
History Depth:          10

Current Prompt:         3COM-DSL>

Local Prompt:           3COM-DSL>
```

show crash_vector

Displays debug information saved after a system crash.

show date

Displays the system *date, time,* and *uptime*. For example:

```
System Date:            09-FEB-2107 15:06:10
System UpTime:          2d 08:37:54
```

show file <filename>

Displays the contents of a text file.

show filter <filter_name >

protocols [BR-ETH]

Displays the filter rules, based on the protocol options specified. The filter name MUST be a filter file, as listed using *list filters*.

- **BR-ETH** - Ethernet bridge data filter rules
- **BR-ETH** - CALL - Ethernet bridge call filter rules

show ethernet counters

Displays counters for the ethernet interface.

INPUT COUNTERS

- **Octets** - bytes received
- **Ucast** - Unicast packets received
- **MultiCast** - Multicast packets received
- **BroadCast** - broadcast packets received
- **Discards** - Number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
- **Errors** - For packet-oriented interfaces, the number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol. For character-oriented or fixed-length interfaces, the number of inbound transmission units that contained errors preventing them from being deliverable to a number of inbound transmission units that contained higher-layer protocol.
- **Unknown Prot** - unknown protocol in packet

OUTPUT COUNTERS

- **Octets** - bytes transmitted
- **Ucast** - unicast packets transmitted
- **MultiCast** - multicast packets transmitted
- **Discards** - Number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
- **Errors** - For packet-oriented interfaces, the number of outbound packets that could not be transmitted because of errors. For character-oriented or fixed-length interfaces, the number of outbound transmission units that could not be transmitted because of errors.
- **Out QLen** - length of the output packet queue (in packets)

show ethernet settings Displays settings for the ethernet interface.

show ip settings Displays system wide IP information.

- **IP System Host Address** - IP address of the system
- **IP Forwarding** – always DISABLED
- **WAN to WAN Forwarding** – indicates if forwarding between WAN Bridge ports is allowed.

show memory Displays System RAM Memory usage.

- **Total System Memory Resources** - total amount of memory in system
- **Free Memory** - amount of memory not in use
- **Code Size** - amount of memory used by code
- **Initialized Data Size**, **Uninitialized Data Size**, **Stack Size** - static data areas

show port <port number> settings Displays the parameters defined for the specified VC. You can use *list vc* to see which virtual channels are defined.

show security_option settings Displays status for SNMP User Access and Administration by Remote Users. You can modify the SNMP User Access using the *enable* or *disable security_option snmp* commands. You can modify Administration by Remote User using the *enable* or *disable security_option remote_user* commands.

- **SNMP User Access** - ENABLED (default) or DISABLED
- **Administration by Remote User** - ON or OFF

show snmp counters Displays many SNMP statistics.

INPUT COUNTERS

- **Packets** - number of SNMP packets received

- **Bad Versions** - SNMP messages for an unsupported SNMP version
- **Bad Community Names** - SNMP messages which used an unknown SNMP community name
- **Bad Community Uses** - SNMP messages which represented an SNMP operation not allowed by the SNMP community named in the message
- **ASN.1 Parse Errors** - sum of ASN.1 or BER errors
- **Too Big Errors** - SNMP PDUs for which the value of the error-status field is 'tooBig'
- **No Such Name Errors** - SNMP PDUs where error-status field is 'noSuchName'
- **Bad Value Errors** - SNMP PDUs where error-status field is 'badValue'
- **Read Only Errors** - SNMP PDUs where the error-status field is 'readOnly'
- **General Errors** - SNMP PDUs where the error-status field is 'genErr'
- **Total Request MIB Objects** - sum of MIB objects retrieved successfully as the result of receiving valid SNMP Get-Request and Get-Next PDUs
- **Total Set MIB Objects** - sum of MIB objects altered successfully as the result of receiving valid SNMP Set-Request PDUs
- **Get Request PDUs** - sum of SNMP Get-Request PDUs accepted and processed
- **Get Next Request PDUs** - sum of SNMP Get-Next PDUs accepted and processed
- **Set Request PDUs** - sum of SNMP Get-Next PDUs accepted and processed
- **Get Response PDUs** - sum of SNMP Get-Response PDUs accepted and processed
- **Trap PDUs** - sum of SNMP Trap PDUs accepted and processed

OUTPUT COUNTERS

- **Packets** - sum of SNMP packets transmitted
- **Too Big Errors** - sum of SNMP PDUs generated by SNMP and for which the value of the error-status field is `tooBig'
- **No Such Name Errors** - sum of SNMP PDUs generated by SNMP and for which the value of the error-status field is `noSuchName'
- **Bad Value Errors** - sum of SNMP PDUs generated by SNMP and for which the value of the error-status field is `badValue'
- **General Errors** - sum of SNMP PDUs generated by SNMP and for which the value of the error-status field is `genErr'
- **Get Request PDUs** - sum of SNMP Get-Request PDUs sent from SNMP
- **Get Next Request PDUs** - sum of SNMP Get-Next PDUs sent from SNMP
- **Set Request PDUs** - sum of SNMP Set-Request PDUs sent from SNMP
- **Get Response PDUs** - sum of SNMP Get-Response PDUs from SNMP
- **Trap PDUs** - sum of SNMP Trap PDUs sent from SNMP

show snmp settings

Displays SNMP settings, which you can modify using *enable* or *disable snmp authentication traps* commands.

- **Authentication Traps** - ENABLED (default) or DISABLED

show system

Displays system information.

- **System Descriptor** - for example:
  3Com HomeConnect™ Remote 810 V1.0.0, Built on Oct 31 1996 at 11:33:05.
- **Object ID** - identifies this system to SNMP managers
- **System UpTime** - time the system has been running since last boot
- **System Contact** - modify using *set system*
- **System Name** - modify using *set system*
- **System Location** - modify using *set system*
- **System Services -** for example, Internet End To End Applications
- **System Version** - loaded version of the system software

show user <name> settings

Displays the parameters defined for the specified TELNET user. You can use *list users* to see which users are defined.

TELNET

TELNET commands are available to users who dial in, and whose *type* is **network** (type parameter in *add user*), whose *host_type* is **prompt** (host_type parameter in *set login user*), and whose *login_service* is **TELNET** (login_service parameter in *set login user*).

telnet <ip_name_or_addr>

Establishes a TELNET client session with the specified IP address.

telnet <ip_addr> TCP_port <number>

Establishes a TELNET client session with the specified IP address using the specified TCP port number. It works just like the TELNET command, except you also specify the TCP port number to be used. The default TCP port number is 23.

UPDATE

The Update Software FTP and Update Software TFTP commands allow you to utilize the 3Com HomeConnect ADSL Modem Ethernet FTP or TFTP clients to obtain and install the new operational software. You can access these commands directly from the serial console CLI session or through TELNET.

To update the software using the FTP command, use the CLI command:

update software ftp <filename>

server <ip_addr>

path <path>

username <username>

password <password>

To update the software using the TFTP command, use the CLI command:

update software tftp <filename> **server <ip_addr> path <path>**

VERIFY

verify filter <filter_name> Verifies the syntax of a filter file, which has been previously *add*ed to the table. If you update a filter file and TFTP it to the FLASH file system, and the file already exists in the filter table, then you use this command to verify the files syntax. You can use *list filters* to see which files are currently in the filter file table, and what the status of each is.

TELNET Commands

The following commands are available to TELNET users. They are accessed by pressing control -].

close Closes the active TELNET connection.

help Lists the available commands

send <string> Transmits a TELNET control character. Be sure the parameters are *uppercase*. The choices are:

Parameters	Description
AYT	Are you there
IP	Interrupt process
BRK	Break
AO	abort output
EC	erase character
EL	erase line
GA	go ahead
NOP	no - operation
EOR	end of record
SYNC	synch

set_escape <string> Allows changing the TELNET escape character from **^]** to something else. Control characters are specified using the carat character followed by another character. For example, to set the TELNET escape character to control - X, type **set_escape ^X**.

status Displays the IP address of the remote host and the value of the TELNET escape character.

CLI Exit Commands

These commands are available to TELNET users so they can disconnect from the CLI.

Bye, Exit, Leave, Quit Leave the CLI, but keep this connection open. This command returns you to the TELNET commands.

Logout Leave the CLI and close this connection. This ends the TELNET session.

Command Features

The command language has several built in features that make it easier to use. When abbreviating commands, it is sometimes hard to remember the commands and their syntax. Using command completion and positional help aids in jogging your memory of the commands and their parameters while you are typing in a command string.

Command Retrieval

Command retrieval retrieves commands from the *history* of previous commands entered. You can display the current command history using the *history* command. You can change the number of commands kept in the command history buffer using the *set command history* command.

^p	recall the previous command in the history list
^n	recall the next command in the history list

Positional Help

Positional help displays the list of possible parameters when you type **?** after any command or parameter . It then redisplays the line you typed, without the **?**, so you can enter the parameter you wish to use. This helps you find the parameter you need, and add it to your command, without having to retype the entire command string. Be sure to leave a space between the keyword and the question mark to use positional help.

Command Completion

The escape key provides command completion. If you press the escape key before you finish typing a command or parameter, the rest of the command or parameter will be displayed (completed), and you can continue entering the command. If the command or parameter is ambiguous, the bell will ding, and the display will not change.

Output Pause

The output will pause when there is more than 24 lines of output. Type ‘more’ (or press CR) to continue, or ‘quit’ to stop.

Command Kill

To discontinue the current command action, and flush any commands which have been typed ahead, use ^C (control-C).

Comments

;	Nothing following a semicolon will be processed. This is useful when you are writing CLI script files. The *do* command runs a CLI script.

TECHNICAL SUPPORT AND LIMITED WARRANTY

Notice: This modem was not designed or approved for use in Europe, Australia, or New Zealand.

Technical Support

3Com provides easy access to technical support information through a variety of services. This section describes those services.

Technical Support Hotline

Technical questions about the 3Com HomeConnect ADSL Modem products can be answered by technical support representatives. This hotline is a toll call.

847-262-3700
8:00am - 6:00pm CST; Monday through Friday

Canadian customers can speak to a technical support representative by contacting Keating Technologies.

905-305-6570
8:00am - 8:00pm EST ; Monday through Friday

Online Technical Support

3Com offers product support 24 hours a day, 7 days a week, through:

World Wide Web	consumer.3com.com/support
3Com BBS	847-262-6000
Email	support@consumer.3com.com

If you need to Return the Modem to Us

Contact 3Com Customer Support. If the support representative determines that you need to return the modem, you will receive an SRO (Service Repair Order) number. You must have an SRO number before returning the modem to us. Ship the unit, postage paid, in a strong box made of corrugated cardboard with plenty of packing material. DO NOT send the modem back in the original box. Send ONLY the modem (NOT manuals, diskettes, etc.) Include your SRO number, name and address on the shipping label as well as inside the package. If possible, send the package via a courier capable of tracking the progress of the shipment. Ship to the following address:

3Com
ATTN: PCD RMA
[your SRO #]
1800 W. Central Avenue
Mount Prospect, IL 60056

Customers in Canada needing to return a modem for repair or replacement should send the modem to the following address:

Keating Technologies
25 Royal Crest Court
Suite 120
Markham, ONT L3R 9X4

Manufacturer's Declaration of Conformity

3Com Corporation
3800 Golf Road
Rolling Meadows, IL 60008
U.S.A.

declares that this product conforms to the FCC's specifications:

Part 15:
Operation is subject to the following two conditions:

(1) this device may not cause harmful electromagnetic interference, and

(2) this device must accept any interference received including interference that may cause undesired operations.

This equipment uses the following USOC jacks: RJ-11C.

Caution to the User

The user is cautioned that any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Part 68:

This equipment complies with FCC Rules Part 68. Located on the bottom of the modem is the FCC Registration Number and Ringer Equivalence Number (REN). You must provide this information to the telephone company if requested.

The REN is used to determine the number of devices you may legally connect to your telephone line. In most areas, the sum of the REN of all devices connected to one line must not exceed five (5.0). You should contact your telephone company to determine the maximum REN for your calling area.

This equipment uses the following USOC jacks: RJ11C.

This equipment may not be used on coin service provided by the telephone company. Connection to party lines is subject to state tariffs.

An FCC compliant telephone cord and modular plug are provided with this equipment, which is designed to connect to the telephone network or premises wiring using a Part 68 compliant compatible jack. See installation instructions for details.

If you have an external modem:

UL Listing/CSA Certified

This information technology equipment is UL-Listed and CSA-Certified for the uses described in the users guide.

If you have an internal modem:

UL Listing/CUL Listing

This information technology equipment is UL-Listed and CUL-Listed for use with UL-Listed personal computers that have installation instructions detailing user installation of card accessories.

Fax Branding

The Telephone Consumer Protection Act of 1991 makes it unlawful for any person to use a computer or other electronic device, including fax machines, to send any message unless such message clearly contains in the margin at the top or bottom of each transmitted page or on the first page of the transmission, the date and time it is sent, an identification of the business or other entity, or other individual sending the message, and the telephone number of the sending machine or of such business, other entity, or individual. (The telephone number provided may not be a 900 number or any other number for which charges exceed local or long-distance transmission charges.)

In order to program this information into your modem, refer to the RapidComm manual on the CD-ROM that shipped with your modem. If you are using a different communication software program, refer to its manual.

Radio and Television Interference

This equipment generates and uses radio frequency energy and if not installed and used properly, in strict accordance with the manufacturer's instructions, may cause interference to radio and television reception. The modem has been tested and found to comply with the limits for a Class B computing device in accordance with the specifications in Part 15 of FCC rules, which are designed to provide reasonable protection against such interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause interference to radio and television communications.

However, there is no guarantee that interference will not occur in a particular installation. If this device does cause interference to radio or television reception, which you can determine by monitoring reception when the modem is installed and when it is removed from the computer, try to correct the problem with one or more of the following measures:

- Reorient the receiving antenna (for televisions with antenna reception only) or cable input device.

- Relocate the computer with respect to the receiver.

- Relocate the computer and/or the receiver so that they are on separate branch circuits.

If necessary, consult your dealer or an experienced radio/television technician for additional suggestions. You may find the following booklet, prepared by the Federal Communications Commission, helpful:

How to Identify and Resolve Radio-TV Interference Problems

Stock No. 004-000-0345-4
U.S. Government Printing Office
Washington, DC 20402

In accordance with Part 15 of the FCC rules, the user is cautioned that any changes or modifications to the equipment described in this manual that are not expressly approved by 3Com could void the user's authority to operate the equipment.

For Canadian Modem Users

Industry Canada (IC)

This digital apparatus does not exceed the Class B limits for radio noise emissions from digital apparatus set out in the interference-causing equipment standard entitled Digital Apparatus, ICES-003 of Industry Canada.

NOTICE: The Ringer Equivalence Number (REN) assigned to each terminal device provides an indication of the maximum number of terminals allowed to be connected to a telephone interface. The termination on an interface may consist of any combination of devices subject only to the requirement that the sum of the Ringer Equivalence Numbers of all devices does not exceed 5.

The Ringer Equivalence Number is located on the bottom of the modem.

Notice

The Industry Canada (IC) label identifies certified equipment. This certification means the equipment meets certain telecommunications network protective, operational, and safety requirements as prescribed in the appropriate Terminal Equipment Technical Requirements document(s). The Department does not guarantee the equipment will operate to the user's satisfaction.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. In some cases, the company's inside wiring associated with a single-line, individual service may be extended by means of a certified connector assembly (telephone extension cord.) The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations. Currently, telecommunication companies do not allow users to connect their equipment to jacks except in precise situations that are spelled out in tariffing arrangements with those companies.

Repairs to certified equipment should be coordinated by a representative designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

For your own protection, make sure that the electrical ground connections of the power utility, telephone lines, and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

CAUTION: Do ***NOT*** attempt to make such connections yourself. Instead, contact an electric inspection authority or electrician, as appropriate.

«AVIS : L'étiquette d'Industrie Canada identifie le matériel homologué. Cette étiquette certifie que le matériel est conforme aux normes de protection, d'exploitation et de sécurité des réseaux de télécommunications, comme le prescrivent les documents concernant les exigences techniques relatives au matériel terminal. Le Ministère n'assure toutefois pas que le matériel fonctionnera à la satisfaction de l'utilisateur.

Avant d'installer ce matériel, l'utilisateur doit s'assurer qu'il est permis de le raccorder aux installations de l'entreprise locale de télécommunication. Le matériel doit également être installé en suivant une méthode acceptée de raccordement. L'abonné ne doit pas oublier qu'il est possible que la conformité aux conditions énoncées cidessus n'empêche pas la dégradation du service dans certaines situations.

Les réparations de matériel homologué doivent être coordonnées par un représentant désigné par le fournisseur. L'entreprise de télécommunications peut demander à l'utilisateur de débrancher un appareil à la suite de réparations ou de modifications effectuées par l'utilisateur ou à cause de mauvais fonctionnement.

Pour sa propre protection, l'utilisateur doit s'assurer que tous les fils de mise à la terre de la source d'énergie électrique, des lignes téléphoniques et des canalisations d'eau métalliques, s'il y en a, sont raccordés ensemble. Cette précaution est particulièrement importante dans les régions rurales.

Avertissement: L'utilisateur ne doit pas tenter de faire ces raccordements lui même; il doit avoir recours à un service d'inspection des installations électriques, ou à un électricien, selon le cas.

Centre de guarantie et de service après-vente:

Keating Technologies
25 Royal Crest Court, Suite 120
Markham, ONT L3R 9X4

3Com Corporation Limited Warranty

3Com warrants this hardware product to be free from defects in workmanship and materials, under normal use and service, for the lifetime of the product from the date of purchase from 3Com or its authorized reseller. 3Com's sole obligation under this express warranty shall be, at 3Com's option and expense, to repair the defective product or part, deliver to Customer an equivalent product or part to replace the defective item, or if neither of the two foregoing options is reasonably available, 3Com may, in its sole discretion, refund to Customer the purchase price paid for the defective product. All products that are replaced will become the property of 3Com. Replacement products may be new or reconditioned. 3Com warrants any replaced or repaired product or part for ninety (90) days from shipment, or the remainder of the initial warranty period, whichever is longer.

YEAR 2000 WARRANTY

In addition to the Warranty stated above, 3Com warrants that each product sold or licensed to Customer on and after January 1, 1998 that is date sensitive will continue performing properly with regard to such date data on and after January 1, 2000, provided that all other products used by Customer in connection or combination with the 3Com product, including hardware, software, and firmware, accurately exchange date data with the 3Com product, with the exception of those products identified at 3Com's Web site,

http://www.3com.com/products/yr2000.html

as not meeting this standard. If it appears that any product that is stated to meet this standard does not perform properly with regard to such date data on and after January 1, 2000, and Customer notifies 3Com before the later of April 1, 2000, or ninety (90) days after purchase of the product from 3Com or its authorized reseller, 3Com shall, at its option and expense, provide a software update which would effect the proper performance of such product, repair such product, deliver to Customer an equivalent product to replace such product, or if none of the foregoing is feasible, refund to Customer the purchase price paid for such product.

Any software update or replaced or repaired product will carry a Year 2000 Warranty for ninety (90) days after purchase or until April 1, 2000, whichever is later.

Obtaining Warranty Service

Customer must contact a 3Com Corporate Service Center or an Authorized 3Com Service Center within the applicable warranty period to obtain warranty service authorization. Dated proof of purchase from 3Com or its authorized reseller may be required. Products returned to 3Com's Corporate Service Center must be pre-authorized by 3Com with a Service Repair Order (SRO) number marked on the outside of the package, and sent prepaid and packaged appropriately for safe shipment, and it is recommended that they be insured or sent by a method that provides for tracking of the package. The repaired or replaced item will be shipped to Customer, at 3Com's expense, not later than thirty (30) days after 3Com receives the defective product. Return the product to:

In The United States:

3Com
USO# _____________
Attn. Dock 15 PCD
1800 W. Central Ave.
Mt. Prospect, IL 60056

In Canada:

Keating Technologies
25 Royal Crest Court, Suite 120
Markham, ONT L3R 9X4

3Com shall not be responsible for any software, firmware, information, or memory data of Customer contained in, stored on, or integrated with any products returned to 3Com for repair, whether under warranty or not.

Warranties exclusive

IF A 3COM PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, CUSTOMER'S SOLE REMEDY FOR BREACH OF THAT WARRANTY SHALL BE REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT 3COM'S OPTION. TO THE FULL EXTENT ALLOWED BY LAW, THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, TERMS, OR CONDITIONS, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES, TERMS, OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, satisfactory quality, CORRESPONDENCE WITH DESCRIPTION, AND NON-INFRINGeMENT, ALL OF WHICH ARE EXPRESSLY DISCLAIMED. 3COM NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE OR USE OF ITS PRODUCTS.

3COM SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THAT THE ALLEGED DEFECT OR MALFUNCTION IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLECT, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO OPEN, REPAIR OR MODIFY THE PRODUCT, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, OTHER HAZARDS, OR ACTS OF GOD.

Limitation of Liability

TO THE FULL EXTENT ALLOWED BY LAW, 3COM ALSO EXCLUDES for itself and its suppliers ANY LIABILITY, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE or profits, LOSS OF BUSINESS, loss of information or data, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF ITS PRODUCTS, even if 3com or its authorized reseller has been advised of the possibility of such damages, AND LIMITS ITS LIABILITY TO REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE paid, AT 3cOM'S OPTION. THIS DISCLAIMER OF LIABILITY FOR DAMAGES WILL NOT BE AFFECTED IF ANY REMEDY PROVIDED HEREIN SHALL FAIL OF ITS ESSENTIAL PURPOSE.

Disclaimer

Some countries, states, or provinces do not allow the exclusion or limitation of implied warranties or the limitation of incidental or consequential damages for certain products supplied to consumers, or the limitation of liability for personal injury, so the above limitations and exclusions may be limited in their application to you. When the implied warranties are not allowed to be excluded in their entirety, they will be limited to the duration of the applicable written warranty. This warranty gives you specific legal rights which may vary depending on local law.

Governing Law

This Limited Warranty shall be governed by the laws of the State of California, U.S.A. excluding its conflicts of laws principles and excluding the United Nations Convention on Contracts for the International Sale of Goods.